Study on application of polar codes to information reconciliation in free-space quantum key distribution

Yuma Yamashita†, Hiroyuki Endo††, Shingo Fujita†, Eiji Okamoto†, Hideki Takenaka††, and Morio Toyoshima††
† Department of Electrical and Mechanical Engineering, Graduate School of Engineering
Nagoya Institute of Technology
†† National Institute of Information and Communication Technology

RESURCH BACKGROUND AND PURPOSE

QKD : quantum key distribution

Background

Satellite-based QKD [1] systems have been attracting much attention to overcome the bottleneck of transmission distance. However, there is a concern that the atmospheric effects may have some impact.

Polar code

① Capacity-achieving performance by channel polarization.
② Low computational complexity in encoding and decoding.
③ Finely configuration by adding or deleting parity bits.

QKD aims to share random numbers
→ the post-processing manner
→ rate-variable error correction

Purpose

Applying a rate-variable error correction based on polar codes to the information reconciliation step for free-space QKD systems.

QUANTUM KEY DISTRIBUTION

XOR : exclusive-OR
QBER : quantum bit error rate

We briefly review the flow of QKD based on the Bennett-Brassard 1984 protocol (BB84) [2], which was the first proposed QKD protocol. In BB84, random numbers are encoded into a single photon's polarization state.

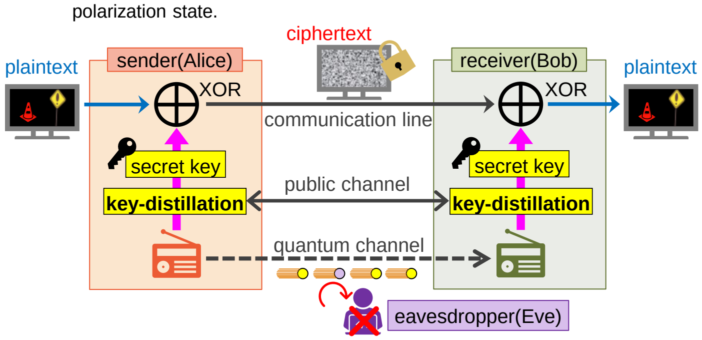

Figure 1. Quantum key distribution.

The key-distillation process roughly consists of (A) QBER estimation, (B) information reconciliation, and (C) privacy amplification.

INFORMATION RECONCILIATION

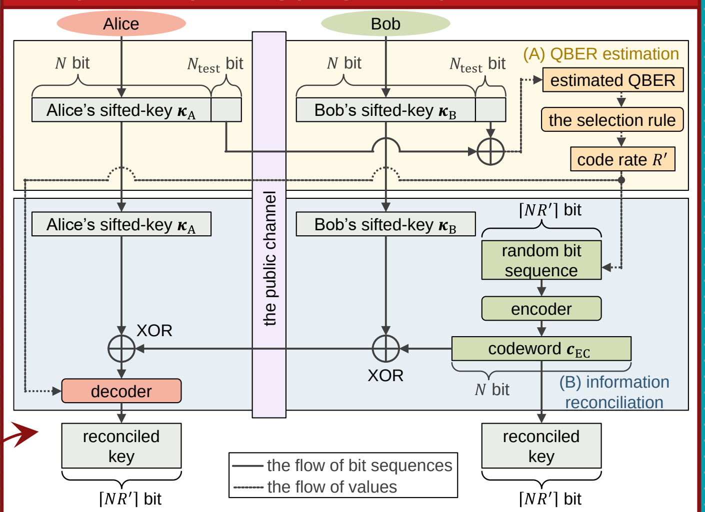

Figure 2. Flow chart for (B) information reconciliation.

NUMERICAL RESULTS

BLER : block error rate
LDPC : low-density parity-check

Performance indicator

$$\left(\frac{\text{the length of the successfully information-reconciliated bit sequence}}{\text{the length of the sifted-key}} \right) = \text{throughput} = R(1 - BLER)$$

Other assumptions

- the errors in the sifted-key are symmetric with respect to the bit 0 or 1, that is binary symmetric channel
- the QBER estimation is assumed to be perfect

Table 1. Simulation conditions of Figure 3.

Code length N_B	2048
Code rate R_{polar}	0.375 to 0.75
Decoding	Successive cancellation list decoding
Parity length of cyclic redundancy check	24

Table 2. Simulation conditions of Figure 4.

LDPC codes	
Code length N_B	2048
Code rate R_{LDPC}	Refer to (2)
Decoding	Sum-product decoding
The maximum number of reprising decoding	20
polar codes	
Code rate R_{polar}	Refer to (1)
The other conditions	Refer to Table1.

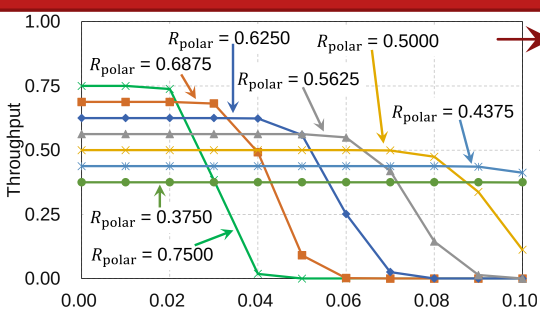

Figure 3. Throughput performances of polar codes.

high-rate polar codes are superior when P_e is small
low-rate polar codes are superior in high P_e region

It is necessary to change the code rate according to P_e for more efficient transmission.

We derived the selection rules for the code rate R_{polar} and R_{LDPC}.

$$R_{polar} = -16507P_e^5 + 7883.2P_e^4 - 1450P_e^3 + 139.25P_e^2 - 10.77P_e + 0.947 \quad (1)$$

$$R_{LDPC} = \begin{cases} 0.750 \ (0 \le P_e < 0.015) \\ 0.625 \ (0.015 \le P_e < 0.044) \\ 0.500 \ (0.044 \le P_e < 0.071) \\ 0.375 \ (0.071 \le P_e < 0.0856) \\ 0.250 \ (0.0856 \le P_e < 0.1) \end{cases} \quad (2)$$

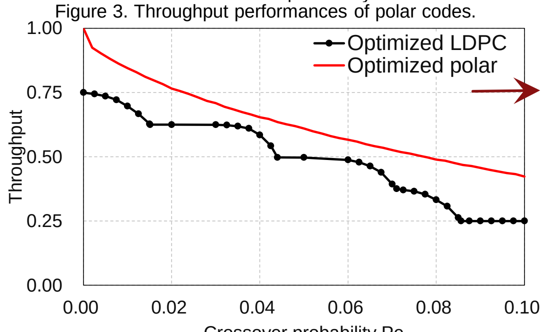

Figure 4. The comparison of optimized throughput performances.

The throughput performances of polar codes are higher than those of LDPC codes in all areas.

The application of polar codes to satellite QKD is expected to improve information reconciliation efficiency.

CONCLUSIONS

We derived a selecting rule of code rate that maximizes throughput for each crossover probability, constructed a polar code with the best throughput performances for information reconciliation, and confirmed the improvement of its performances.

[1] R. Bedington, et al., *npj Quantum Information* 3, (2017).
[2] C. H. Bennett, et al., *Proc. of IEEE Int'l Conf. on Computers, Systems and Signal Proc., Bangalore India*, 175-179 (1984).